Gestión Joven
Revista de la Agrupación Joven Iberoamericana de Contabilidad y Administración de Empresas (AJOICA)

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

Gestión de la privacidad de datos sensibles. El aplicativo CuidAR para el control del COVID-19

Natalia Romina Salaberry
Facultad de Ciencias Económicas.
Universidad de Buenos Aires.
natyeconomia@economicas.uba.ar

Pablo Matías Herrera
Centro de Investigación en Metodologías Básicas y Aplicadas a la Gestión (CIMBAGE, IADCOM, Facultad de Ciencias Económicas).
Universidad de Buenos Aires.
pabloherrera@economicas.uba.ar

RESUMEN

El presente trabajo tiene por objetivo analizar la gestión de la privacidad de datos sensibles (personales, de salud y de geolocalización) en el uso de aplicativos móviles tomando como referencia el caso de Argentina. La utilización de aplicativos móviles para el control de la pandemia del COVID-19 ha puesto de manifiesto la granularidad de la información recopilada lo que representa un riesgo en la privacidad de su titular. Esta es concebida como el derecho que tiene un individuo para poder controlar sus propios datos. En este contexto, la elaboración de una taxonomía de los diferentes tipos de aplicativos existentes -entrando en un análisis más detallado en el caso de la aplicación CuidAR de Argentina- resulta oportuno para poder identificar con mayor claridad los riesgos asociados en torno a esta. A su vez, la definición de la privacidad desde una concepción diferencial se presenta como una posible solución al tratamiento de datos sensibles.

El recorrido realizado a lo largo de este trabajo no agota todas las posibilidades, sino que intenta reconocer la existencia de una problemática vigente ofreciendo una posible solución. Como resultado las organizaciones, en particular las públicas, podrán contar con un mayor caudal de información sin que se incurra en una violación del derecho a privacidad de sus titulares generando un mayor nivel de confianza entre los usuarios y esta.

Palabras clave: Datos sensibles, Privacidad de datos, Aplicativos móviles, Coronavirus, CuidAR

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

ABSTRACT

The present work aims to analyze the management of the privacy of sensitive data (personal, health and geolocation) in the use of mobile applications, taking the case of Argentina as a reference. The use of mobile applications to control the COVID-19 pandemic has revealed the granularity of the information collected, which represents a risk to the privacy of its owner. This is conceived as the right that an individual has to control their own data. In this context, the development of a taxonomy of the different types of existing applications - entering into a more detailed analysis in the case of the CuidAR application in Argentina - is appropriate to be able to more clearly identify the risks associated with it. In turn, the definition of privacy from a differential conception is presented as a possible solution to the processing of sensitive data.

The route carried out throughout this work does not exhaust all the possibilities, but rather tries to recognize the existence of a current problem by offering a possible solution. As a result, organizations, particularly public ones, will be able to count on a greater flow of information without incurring a violation of the right to privacy of their holders, generating a higher level of trust between users and the latter.

Key words: Sensitive data, Data privacy, Mobile applications, Coronavirus, CuidAR

INTRODUCCIÓN

A partir del desarrollo tecnológico de las últimas dos décadas, la digitalización de la comunicación se ha convertido en un espacio generador de grandes volúmenes de datos. La posibilidad de contar con estos de manera dinámica e inmediata para la toma de decisiones ha despertado un interés entusiasta en las organizaciones. Un ejemplo de actualidad es el uso de aplicativos móviles (Apps) como herramienta de control de la pandemia del COVID-19 por parte de Autoridades Nacionales en diferentes países. Esta modalidad ha despertado controversias acerca de cómo está siendo protegida la privacidad de sus usuarios, frente a la recopilación y almacenamiento de datos sensibles (personales, de salud y de geolocalización).

Los diferentes tipos de aplicativos dejan entrever los riesgos asociados que surgen en torno a la privacidad de datos. Para poder identificarlos, en el primer aparatado se realiza una taxonomía de los diferentes tipos de Apps, clasificándolos en cuatro grandes grupos. Si bien cada uno presenta un objetivo en particular, comparten un factor en común: recopilan, procesan y almacenan datos sensibles de sus usuarios. El resultado de este proceso implica, entre otros, la geolocalización del titular de los datos. Si bien puede resultar una medida necesaria para controlar la propagación del virus, no deja de ser una invasión a la privacidad de los individuos despertando controversias acerca de la utilización de esta tecnología.

Argentina es uno de los países en los que se ha implementado el uso de este tipo de aplicativos. Las Autoridades Nacionales pusieron a disposición de la ciudadanía el aplicativo CuidAR para auto testeo de síntomas y control de cumplimiento de aislamiento social obligatorio en caso de haber sido diagnosticado positivamente con la enfermedad. En el segundo apartado se realiza un análisis a partir de los términos y condiciones de esta. Además de poder conocer cuáles son específicamente los datos recopilados, entre otros, constituye un ejemplo de cómo los usuarios dejan en manos

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

del Gobierno sus datos ante las exigencias de las Autoridades. En este sentido se abre un debate en torno a la privacidad que puede llegar a extremo, aunque no es exclusivo de la sociedad argentina. Sino que se ubican en un debate vinculado al desarrollo tecnológico a nivel mundial.

Frente a un escenario tan controversial en torno a la privacidad de datos, en el tercer apartado se realiza un análisis desde una visión regulatoria. Si bien la regulación existente puede brindar un reparo para los usuarios de este tipo de tecnologías, no resulta suficiente respecto de los riesgos asociados. Ante ello se propone la construcción de la privacidad a partir del concepto de privacidad diferencial, estableciéndola desde el diseño. Esto permitirá gestionar el riesgo de manera proactiva para establecer una estrategia que incorpore a la protección de datos durante todas las etapas del procesamiento. Como resultado, se podrá contar con mayor cantidad de información sobre la población siendo un impacto positivo, lo que permitirá realizar un control más acabado en situaciones como la actual pandemia del coronavirus.

1. LA PANDEMIA DEL COVID-19 Y LOS APLICATIVOS MÓVILES PARA SU CONTROL

Desde fines de 2019, el mundo se encuentra afectado por la rápida expansión de un virus. El virus se conoce con el nombre de SARS-CoV-2, a partir de que la International Committee on Taxonomy of Viruses (ICTV) logra identificar su taxonomía y establece su nombre (Liu, Kuo y Shih, 2020). El 12 de enero de 2020, la Organización Mundial de la Salud (OMS) nombra temporalmente al virus como Nuevo Coronavirus 2019 (2019-nCov). El 12 de febrero de 2020, lo denomina oficialmente enfermedad infecciosa bajo el nombre de Coronavirus 2019 (COVID-19). A partir de entonces, el virus comienza a ser denominado COVID-19 alcanzando a diferentes ciudades del mundo. El 11 de marzo de 2020 la OMS lo declara una pandemia.

Frente a este escenario, las autoridades nacionales de cada país han adoptado diferentes medidas con el fin de poder controlar la expansión de la pandemia. Las medidas adoptadas, en muchos casos, contaron con el apoyo de herramientas tecnológicas en un contexto donde las sociedades modernas se caracterizan por estar continuamente conectadas. La recolección de datos a partir de dispositivos tecnológicos modernos se ha convertido de interés para las organizaciones. En particular, las organizaciones públicas se muestran entusiastas con la posibilidad de contar con datos que le permiten tomar decisiones de una manera dinámica (Gasser, Ienca, Scheibner, Sleigh y Vayena. 2020).

De las diversas tecnologías existentes la modalidad de prestación de servicios a través de aplicativos (Apps), móviles o web, se ha convertido en la predilecta para afrontar el avance de la pandemia. Una Apps es un software particular que, dadas sus características, permite realizar diversos tipos de funciones. Para el control de la pandemia, la característica de las Apps que resulta de interés es su capacidad de procesar grandes cantidades de datos personales. Cantú, Cheng, Doerr, Frost, y Gambacorta (2020) proponen una taxonomía que clasifica las Apps desarrolladas en el contexto de pandemia de acuerdo con su funcionalidad.

El primer tipo de aplicativo tiene por objetivo brindar atención médica para diagnóstico en forma remota. Esto permite descongestionar los centros de salud, disminuyendo el

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

riesgo de colapso de estos. Ejemplos de este tipo de Apps son “moveUP App” de Bélgica o la App “CuidAR” de Argentina (Azevedo, 2020). El segundo tipo de aplicativos tiene por objetivo brindar información general sobre la evolución de la pandemia. Entre los de este tipo, se encuentran los que evalúan flujos de circulación de personas en forma agregada por determinadas zonas geográficas. La App “Coronavirus SUS” de Brasil es un ejemplo de estos. Un tercer tipo, tiene por objetivo llevar a cabo un control más acabado sobre el cumplimiento del aislamiento social obligatorio sobre aquellas personas que regresan de un país de alto riesgo de contagio. Este tipo de Apps utiliza la geolocalización de la persona solo con el objeto de asegurar que la persona cumpla con la restricción. “GeoHealthApp” de Alemania o “StayHomeSafe” de China son ejemplos de esta categoría. El cuarto tipo de aplicativo se focaliza en controlar la transmisión comunitaria del virus. Para este propósito, se realiza un rastreo de contactos de la persona con riesgo de haber contraído la enfermedad o que ya fue diagnosticada con la misma. Con esta información se alerta a otros usuarios. Un ejemplo es la App “Corona Map” de Corea del Sur.

Un factor en común entre los diferentes tipos de aplicativos resulta en la recopilación, procesamiento y almacenamientos de datos sensibles (personales, de salud y de geolocalización) de los usuarios. Mientras los dos primeros tipos mencionados recopilan datos principalmente personales y de salud de sus usuarios, los últimos dos casos se focalizan en la recopilación de datos personales y de geolocalización. Con datos personales se refiere a aquellos que describen atributos de un individuo identificado, o que permiten realizar una individualización e identificación única de este. Los datos de salud surgen de respuestas que brindan los usuarios a preguntas relacionadas con evaluación de síntomas sobre COVID-19. En cambio, los datos de geolocalización se obtienen a través del Global Positioning System (GPS) de los dispositivos móviles a través del es utilizada la App.

A medida que se avanza en el objetivo del control de la pandemia, la necesidad de geolocalizar a los usuarios se incrementa. Los datos sensibles que se proveen en las Apps, en particular los de salud y de geolocalización, permiten la identificación de sus usuarios. En este punto se visibilizan controversias en cuanto a la privacidad de estos. En el caso de los aplicativos de autoevaluación de síntomas de COVID-19, los datos de salud recopilados son transferidos a través de otros canales a las Autoridades de Salud correspondiente para que personal idóneo pueda dar certeza sobre el diagnóstico. Además, en algunos casos, es utilizada la geolocalización para controlar el cumplimiento del aislamiento social obligatorio. Argentina cuenta con un aplicativo de este tipo, denominado CuidAR[1] — creada por la Secretaría de Innovación Pública, el Ministerio de Ciencia y Tecnología de la Nación, la Fundación Sadosky, el Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) y la Cámara de la Industria Argentina del Software (CESSI), que nucleó a las empresas Hexacta, Globant, G&L Group, C&S, QServices, GestiónIT, Intive, Finnegans y Faraday. Asimismo, el equipo se complementó con el trabajo de Arsat, la empresa de telecomunicaciones del Estado, y los servicios brindados por Amazon Web Services, RedHat Argentina, Thinkly y Biodyn SAS—.

[1] La App se encuentra disponible en su versión web –accesible a través de argentina.gob.ar/coronavirus– como en su versión para dispositivos móviles que podrá descargarse de las tiendas de aplicaciones oficiales de Android e iOS.

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

2. EL CASO DE LA APLICACIÓN CUIDAR EN ARGENTINA

El 24 de marzo de 2020 las Autoridades Nacionales de Argentina puso a disposición de la sociedad una aplicación que sirve para realizarse una autoevaluación de síntomas del virus COVID-19, así como obtener asistencia o recomendaciones en caso de compatibilidad con este, denominada CuidAR. Esta decisión forma parte del conjunto de medidas adoptadas frente a la expansión de la pandemia en el territorio nacional, con el fin de poder brindar respuesta sanitaria en contexto pandémico. A continuación, se realiza una descripción a partir de sus términos y condiciones[2].

La Aplicación CuidAR (en adelante App) es una herramienta tecnológica que brinda información a quien la utilice (usuario) sobre diversos temas referentes a los síntomas y/o prevención del virus COVID- 19 con la finalidad de ayudar a prevenir la propagación del virus. El usuario, a partir de la respuesta que brinda a preguntas relacionadas con su estado de salud y sintomatología compatible con el virus, recibirá orientación y/o instrucciones para ser atendido en la unidad de salud más cercana. Para ello, la App recopila datos con el objetivo de que las organizaciones de gobierno lleven adelante políticas públicas de prevención y mitigación relacionadas con el virus y con la emergencia declarada. Para este fin, las organizaciones de gobierno —representadas por la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros de la Nación [3] (en adelante, la "Secretaría")— utilizan la información suministrada por el usuario de acuerdo con lo explicitado en los términos y condiciones. Los términos y condiciones de la App se dividen en diferentes apartados y, el quinto en particular refiere a la protección de los datos personales y su política de privacidad. Se abarca todo lo relacionado con tratamiento de los datos que realiza la Secretaría, aclarando que los términos y condiciones están en línea con lo dispuesto por la Ley de Protección de Datos Personales y Habeas Data Nº 25.326. De esta ley se toman definiciones vinculadas con la clasificación y el procesamiento de los datos[4] y se hace explícito el cumplimiento de los principios que surgen de la Normativa de Protección de Datos Personales[5] por parte de la Secretaría.

Frente al hecho de que los datos se dejan en manos del Gobierno, al aceptar los términos y condiciones, el usuario presta su consentimiento expreso para que la Secretaría trate los datos personales (incluyendo, pero sin limitarse al nombre, DNI, CUIT/CUIL, edad, domicilio, e información referida a su salud tal como síntomas, antecedentes médicos y diagnóstico) que el usuario declare, como así también información de geolocalización que la Aplicación recolecte en forma automatizada. Para acceder a la información de geolocalización, la Aplicación utilizará el GPS de los dispositivos móviles. La finalidad específica de la recolección de estos es la recomendación de medidas preventivas, activar los sistemas de emergencia para brindar asistencia sanitaria, conectar al usuario con un centro de asistencia sanitaria cercano y realizar mediciones y predicciones basadas en recomendaciones sanitarias

[2] Los términos y condiciones no están exentos de la dinámica del aplicativo. En este sentido, en un principio la aplicación estaba sujeta a los término y condiciones de los Servicios Digitales en general. Por las especificidades de la aplicación, se han desarrollado términos y condiciones propios del aplicativo teniendo en cuenta los término y condiciones de los Servicios Digitales.

[3] Organismo encargado del desarrollo de aplicaciones móviles oficiales (entre otros servicios digitales) del Estado Nacional con fines diversos.

[4] Datos personales, datos sensibles, base de datos, tratamiento de datos, responsable de la base de datos, datos informatizados, titular de los datos, usuario de datos y disociación de datos.

[5] Principio de legalidad, principio de calidad, principio de finalidad, principio del consentimiento informado y principios de seguridad y confidencialidad de la información.

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

por parte del Ministerio de Salud de la Nación. De esta manera se habilita la posibilidad de construir mapeos de zonas de riesgo, entre otras.

En cuanto a los datos personales, el consentimiento expreso del usuario habilita a la Secretaría a ceder los datos a otras entidades estatales y/o establecimientos sanitarios nacionales, provinciales o municipales, para que estos también puedan mitigar la propagación del virus COVID-19 y colaborando en la prevención de la sobreocupación del sistema sanitario. De esta manera, las organizaciones de gobierno persiguen dos fines. El primero es recomendarle al usuario los pasos a seguir según su situación e instrucciones para ser atendido en la unidad de salud más cercana. El segundo es realizar comparaciones y predicciones, basadas en recomendaciones sanitarias que determine el Ministerio de Salud de la Nación.

Dentro de los términos y condiciones se aclara que los datos personales que el usuario suministre a través de la App, como así también los que la App recolecte en forma automatizada serán almacenados en una base de datos de la cual se responsabilizan las organizaciones de gobierno [6] . La permanencia en forma almacenada de estos será conservada únicamente mientras sean necesarios y dure la emergencia sanitaria. Una vez finalizada esta, podrán conservarse solo versiones anonimizadas de los mismos con fines científicos y epidemiológicos.

La sensibilidad de los datos aportados por el usuario mediante el uso de la App y las exigencias que las Autoridades Nacionales realizan sobre su utilización ha abierto una serie de cuestiones. Estos cuestionamientos no son exclusivos de la sociedad argentina, sino que se ubican en un debate vinculado al desarrollo tecnológico a nivel mundial. Al tratarse del uso de tecnología basada en datos sensibles, las Autoridades Nacionales argumentan su utilización basandose en el apoyo que la Organización Mundial de la Salud y la Organización Panamericana de la Salud realizan con este fin. Si bien los organismos mencionados apoyan la utilización de estas tecnologías con fines de Salud, también advierten sobre la necesidad de establecer un contexto seguro y acorde (World Health Organization, 2019) para evitar riesgos cuando se hace uso de los datos o se los transfiere. Es, entonces, que se comienza a cuestionar como están siendo protegidos por parte de las organizaciones.

Los cuestionamientos en torno a la privacidad de datos sensibles recopilados a través de aplicativos móviles han abierto debates que llegan a ser extremos, como aquellos que plantean la necesidad de elección entre privacidad o salud. Es por ello por lo que entender la problemática entorno a esta resulta de importancia y necesidad. De esta manera se podrá evaluar la posibilidad de establecer un marco de privacidad que garantice la protección de datos en tanto derecho que poseen los individuos.

3. LA PRIVACIDAD DE DATOS EN APLICATIVOS MÓVILES PARA EL CONTROL DE LA PANDEMIA

Si bien el desarrollo de la tecnología para ayudar a contener la expansión del COVID-19 permite mantener el valor de la efectividad en término de políticas públicas, también desafía ciertos valores que requieren ser repensados de manera dinámica. En particular, el desarrollo de las Apps y su característica de procesar grandes volúmenes de datos personales de forma instantánea pone de manifiesto la necesidad de

[6] En particular, se mencionan a la Subsecretaría de Gobierno Abierto y País Digital de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros de la Nación.

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

replantear y reflexionar acerca del valor que la sociedad le confiere a la privacidad. Si a la privacidad se la considera como un valor, entonces, se deben considerar ciertas reglas para regular las acciones que lo interpelen.

La privacidad es un derecho humano universal que refiere a que todo individuo tiene derecho a vivir en privacidad. Este derecho, contenido en el artículo 12[7] de la Declaración Universal de los Derechos Humanos de 1948, alcanza a los datos sensibles que forman parte de la vida privada. Sin dudas, el desarrollo de las tecnologías que permiten procesar grandes volúmenes de datos interpela este derecho. En un escenario dinámico en cuanto al desarrollo de tecnologías vinculadas con las Apps y su potencial de procesar grandes cantidades de datos personales, también se han realizado diferentes acciones para preservar la privacidad como un derecho. A continuación, se describen algunas de estas acciones que permiten visibilizar la valorización de la privacidad en diferentes partes del mundo y se presenta una metodología que permite preservar este valor.

La Unión Europea cuenta con un marco regulatorio de privacidad denominado Reglamento General de Protección de Datos (GDPR) —que entra en vigor en mayo de 2018— y se ha convertido en un referente mundial. Uno de los elementos esenciales que se establece en este es que el consentimiento es la base de la gestión de datos personales (Buenadicha, Galdon, Hermosilla, Loewe, y Pombo, 2019). Esto implica que, además de las cuestiones entorno a la seguridad, quienes recolecten y gestionen los datos deberán asegurarse siempre de haber informado a sus propietarios (los individuos) y obtener su consentimiento tantas veces como sea necesario si la finalidad del uso que se le dará cambia. Además de respetar el derecho a privacidad de los individuos, esta noción constituye un eje fundamental del contrato social que permite generar confianza entre quienes los proporcionan y quienes los manejan.

En el caso de Estados Unidos de América cada estado cuenta con sus propias leyes de protección al consumidor sin que exista una ley o marco regulatorio nacional de protección de datos. Si bien el gobierno nacional ofrece una serie de recomendaciones[8] acerca de cómo protegerlos y se recomienda consultar a la agencia estatal de su estado, la responsabilidad sobre la protección de la información queda depositada en manos del individuo. Dada esta situación y en el contexto actual del uso de aplicativos móviles para el control de la pandemia, se han reunido diferentes expertos y representantes de las universidades más importantes del país[9] para exponer los riesgos asociados a la violación de la privacidad que conlleva el uso de la mencionada tecnología. Esto con el fin de que se tomen acciones regulatorias en este sentido.

China ha sido el primero que comienza a utilizar tecnología móvil para el control de la pandemia. Si bien cuenta con una ley de protección de datos personales —denominada “Cybersecurity Law of the People’s Republic of China” (CSL)[10] —, las autoridades nacionales no son las responsables de velar por el cumplimiento de esta.

[7] Art. 12: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.” Organización de las Naciones Unidas. Declaración Universal de Derechos Humanos.
[8] Véase usa.gov. Accesible a través de https://www.usa.gov/espanol/proteja-su-privacidad
[9] Para mayor detalle véase IMPACT 2020. Accesible a través de https://pact.mit.edu/impact-2020/
[10] Véase ICLG.com. Accesible a través de https://iclg.com/practice-areas/data-protection-laws-and-regulations/china

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

Sino que la Administración del Cyber Espacio es la encargada de coordinar la Cyber Seguridad y otros departamentos son los responsables de su supervisión. De esta manera, la responsabilidad queda nuevamente en manos del individuo sin contar con una regulación estricta.

En este contexto mundial, Argentina cuanta con la Ley 25.326 de Protección de Datos Personales[11] sancionada en el año 2000. La ley busca velar por el derecho al honor y a la intimidad de las personas conforme al artículo 43 párrafo tercero de la Constitución Nacional. Alcanza a los titulares de los datos personales, pero también a quienes hacen uso de estos indicando la obligación de realizar una disociación de manera que la información obtenida no pueda asociarse a una persona determinada. Si bien, se establece (Art. 5°) la necesidad de contar con el consentimiento expreso del titular de los datos personales para hacer uso de estos, también se establecen excepciones. Entre las excepciones, se encuentra el caso cuyo fin es el ejercicio de funciones propias de los poderes del Estado. En este sentido se indica sólo pueden ser recolectados y ser objeto de tratamiento cuando medien razones de interés general autorizadas por ley. En el caso particular de los datos de salud, los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectarlos y tratarlos respetando los principios del secreto profesional.

A pesar de la regulación vigente en cada país, los diferentes tipos de aplicativos dejan entrever los riesgos asociados que surgen en torno a la privacidad de datos. En el caso de los aplicativos que utilizan la geolocalización de los usuarios para realizar rastreo de contactos, resulta cuanto menos invasivo de la privacidad. Pero, además, implica que el usuario tenga que activar el Bluetooh[12] de su dispositivo continuamente exponiéndose a un riesgo de robo de datos (Gasser, Ienca, Scheibner, Sleigh, & Vayena, 2020). En cambio, los dispositivos que utilizan la información obtenida del GPS en forma agregada resultan menos invasivos. Sin embargo, el nivel de granularidad de la información recolectada pone de manifiesto el riesgo de reidentificación de su titular.

Por otra parte, aquellos que recopilan datos personales y de salud, también utilizan la geolocalización de los usuarios. Si bien, informan flujos de circulación de manera agregada por zonas geográficas, no hay una explicación transparente acerca de cómo es procesada y almacenada la información. Los que tienen por objeto principal el diagnóstico también resultan de uso obligatorio para quienes deben aislarse por tiempo determinado ante un diagnóstico positivo de COVID-19. Entre este tipo, se encuentra la App CuidAR de Argentina. Cuando un individuo es diagnosticado positivamente con el virus para controlar que cumpla con el aislamiento obligatorio debe utilizarla. Si bien no resulta claro que la aplicación realice un rastreo activo del individuo, el hecho de controlar su ubicación física no deja de ser un rastreo del paradero de este. Además, tampoco es claro cómo se lleva a cabo la transferencia de datos a las Autoridades de Salud según corresponda el caso. Esta situación no hace más que despertar desconfianza acerca de cómo están siendo protegidos los datos.

Por lo tanto, la legislación establece el deber ser ante la cual el usuario puede ampararse. Pero no se ocupa del cómo ha de llevarse a cabo la construcción de la

[11] Art 2°: “Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.” Tomado de InfoLEG. Accesible a través de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm
[12] Tecnología de comunicación y transferencia de datos entre dispositivos de corto alcance.

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

privacidad en la tecnología. Si bien el control de la pandemia proporciona razones suficientes para ponerla en segundo lugar, surge la necesidad de establecer reglas claras que regulen la protección de los datos y la posibilidad de su reutilización en otros contextos. Una posibilidad viene dada por la concepción de la privacidad diferencial (Dwork, 2008). Como resultado se obtendrá una cierta distorsión en los datos, aunque permitirá que un análisis posterior no se vea sustancialmente afectado. Si no, brinda la posibilidad de contar con un método matemático[13] riguroso para hacer frente a la posibilidad de reidentificación del titular. No obstante, requerirá de la evaluación de un costo que vendrá dado por cuanta información real se está dispuesto a no publicar o utilizar a cambio de obtener privacidad. En consecuencia, esta será construida desde el diseño (Agencia Española de Protección de Datos, 2019).

El enfoque de la privacidad desde el diseño significa, entonces, gestionar el riesgo de manera proactiva para establecer una estrategia que incorpore a la protección de datos durante todas las etapas del procesamiento. Esto permitirá que las responsabilidades sean asignadas por defecto, informando y formando a quienes se encuentren involucrados en cada una de estas. De esta manera, se determinará qué datos sensibles son los necesarios para cada fin específico definiendo una gestión responsable. Pero, además, dada la diversidad de estos, se requerirá del diseño de un plan de gobierno de datos que permitirá una articulación entre todas las áreas de la organización para delinear adecuadamente una estructura de datos sólida (McKeen y Smith, 2008).

Como resultado, la organización podrá contar con mayor cantidad de información sobre la población siendo un impacto positivo, ya que les permitirá realizar un control más acabado en situaciones como la actual pandemia del coronavirus. Para lograrlo, las personas de cada área deberán asumir responsabilidad frente a cualquier situación adversa sobre la calidad de los datos, al mismo tiempo que deberán brindar confiabilidad sobre estos. Esta última, vendrá dada por la prevención de la fuga de información o la violación en la privacidad de esta (Kim y Cho, 2018). De esta manera, se podrán evitar que ocurran hechos como el caso de la web del Gobierno de San Juan para tramitar permisos de circulación lo cual marca un antecedente. Por error fueron expuestos —con libre acceso a través del código HTML (HyperText Markup Language)— los datos sensibles de 115 mil ciudadanos que habían tramitado uno de estos[14].

A pesar de las dificultades que pudiesen surgir entorno al uso de estas tecnologías, no dejan de constituir una herramienta muy útil para las Autoridades Nacionales en el control de la pandemia. Por esta razón se considera necesario la asignación de responsabilidades sobre quienes gestionen cada una de las etapas del procesamiento de los datos, asegurándole a los ciudadanos la disminución del riesgo en su privacidad. Esto facilitará generar un mayor grado de confianza con las organizaciones, en particular las públicas, lo que se traducirá en más información disponible para la toma de decisiones.

[13] Para mayor detalle del modelo véase Dwork, C. (2008, April). Springer, Berlin, Heidelberg.
[14] Para más información del caso véase en Comparitech: Argentina health officials expose personal data on 115,000 COVID-19 quarantine exemption applicants. Disponible en https://www.comparitech.com/blog/information-security/argentina-covid-permit-data-leak/

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

CONCLUSIÓN

Los aplicativos móviles se posicionan como una herramienta tecnológica favorable para el control de la pandemia del COVID-19. Pero a su vez ponen de manifiesto los riesgos asociados a la privacidad de datos que recopilan, entendiendo por esta al derecho que tiene un individuo de poder ejercer un control sobre sus propios datos. Frente a este escenario surgen posiciones extremas que plantean la elección entre privacidad o salud. Ante tal disyuntiva en este trabajo se realizó un abordaje en torno a la privacidad de datos para brindar una posible solución intermedia. A partir de establecer una taxonomía sobre los diferentes aplicativos se logra dar cuenta de los riesgos asociados en torno a esta.

La recopilación de datos sensibles (personales, de salud y de geolocalización) que realiza cada tipo de aplicativo, pone de manifiesto los riesgos asociados en torno a privacidad de los titulares de estos. Por ejemplo, geolocalizar un individuo implica determinar su ubicación física resultando en una identificación de este. Esto constituye una violación a su privacidad. Al mismo tiempo, en el contexto actual -afectado por el virus COVID-19- las Autoridades nacionales requieren poder ejercer un control sobre la expansión de la pandemia de forma tal de evitar la mayor cantidad de contagios posible. Para ello se apoyan en la utilización de este tipo de tecnología.

Si bien existe legislación sobre la privacidad de datos en la gran mayoría de los países, puede no resultar suficiente para dar garantía eficaz en el procesamiento de datos. Surge entonces la propuesta de tratarla desde el concepto de Privacidad Diferencial. Este permitirá establecer cuanta información real se está dispuesto a no publicar o utilizar a cambio de obtener privacidad. A su vez, se requerirá de una gestión adecuada. Una posibilidad que se presenta es establecer a la privacidad desde el diseño. A partir de esta se podrá gestionar el riesgo de manera proactiva durante todas las etapas del procesamiento de los datos, permitiendo que las responsabilidades sean asignadas por defecto, informando y formando a quienes se encuentren involucrados en cada una de estas. Como resultado se podrá obtener un caudal de información más amplio para la toma de decisiones al mismo tiempo que se establecerá un mayor grado de confianza entre los usuarios y las organizaciones.

En un contexto donde los cambios tecnológicos conllevan una dinámica constante, esta propuesta no agota todas las posibilidades. La problemática sobre privacidad de datos no es exclusiva de un país en particular, sino que se ubican en un debate vinculado al desarrollo tecnológico a nivel mundial. En este sentido, resulta de interés llevar adelante una ampliación de este trabajo que permita abordar diferentes experiencias internacionales permitiendo evaluar diversas soluciones posibles.

Vol. 22 - Núm. 2 - 2021
ISSN 1988-9011
pp. 48 - 58

BIBLIOGRAFÍA

Agencia Española de Protección de Datos (2019). Guía de Privacidad desde el Diseño. Sede Electrónica: https://www.aepd.es/es

Azevedo Silva, M. EENA (2020). "COVID-19 Apps". European Emergency Number Association EENA 112. Brussels, Belgium.

Buenadicha, C., Galdon, G., Hermosilla, M. P., Loewe, D., & Pombo, C. (2019). La Gestión Ética de los Datos. Por qué importa y cómo hacer un uso justo de los datos en un mundo digital BID, editor.

Cantú, C., Cheng, G., Doerr, S., Frost, J., & Gambacorta, L. (2020). On health and privacy: technology to combat the pandemic (No. 17). Bank for International Settlements.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. Communications of the ACM, 42(2), 60-67.

Dwork, C. (2008, April). Differential privacy: A survey of results. In International conference on theory and applications of models of computation (pp. 1-19). Springer, Berlin, Heidelberg.

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020). Digital tools against COVID-19: Framing the ethical challenges and how to address them. arXiv preprint arXiv:2004.10236.

Kim, H. Y., & Cho, J. S. (2018). Data governance framework for big data implementation with NPS Case Analysis in Korea. Journal of Business and Retail Management Research, 12(3).

Liu, Y. C., Kuo, R. L., & Shih, S. R. (2020). COVID-19: the First Documented Coronavirus Pandemic in History. Biomedical Journal.
McKeen, J. D., & Smith, H. A. (2007). Developments in practice XXIV: information management: the nexus of business and IT. Communications of the Association for Information Systems, 19(1), 3.

World Health Organization. (2019). WHO guideline: recommendations on digital interventions for health system strengthening: web supplement 2: summary of findings and GRADE tables (No. WHO/RHR/19.7). World Health Organization.